Internet of Things and Cloud Computing
2018; 6(1): 12-16
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.20180601.12
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

Security Enhancement in Multi Clouds Using Serverless Computing Approach

R. Poorvadevi, S. Ramamoorthy

Department of Computer Science and Engineering, Sri Chandra Sekharendra Saraswathi Viswa Maha Vidhyala (SCSVMV) University, Kanchipuram, India

Email address:
poorvadevi@gmail.com (R. Poorvadevi), sriraram2@gmail.com (S. Ramamoorthy)

To cite this article:
R. Poorvadevi, S. Ramamoorthy. Security Enhancement in Multi clouds Using Serverless Computing Approach. *Internet of Things and Cloud Computing*. Vol. 6, No. 1, 2018, pp. 12-16. doi: 10.11648/j.iotcc.20180601.12

Received: January 18, 2018; **Accepted**: February 1, 2018; **Published**: March 14, 2018

Abstract: Nowadays, in any application specific domain security plays a vital role in the service access environment. Because customers needs to make use of distinct services and resources in an attacks free surface. In cloud computing environment, the security services and portal systems have been highly progressed based on the user requirements. However, cloud offers plenty of resources through the service vendor globally; still the multi clouds problems are not resolved completely. So, it is very essential to protect the data and other resources from the intruders are a most primary factor. The proposed work will establish a security layer on the multiple cloud environments by introducing the concept of "Serverless Computing". The serverless computing is a kind of cloud computing execution model through which the cloud service provider (CSP) can manage the allocation of system resources in a dynamic manner. This mechanism will follow the property of utility computing. This approach can be used to hide the operations on entire cloud server management end and capacity planning decisions and also uses no provisioned services. Any type of vulnerabilities is taken care of by the cloud service provider. In this process, attacks rate are compared with the traditional security architectures and each component is an entry point to the serverless application. With this approach, customers can control and monitor the workloads by using IDS / IPS technique.

Keywords: Cloud User, Cloud Service Provider, Virtual Machine, Virtual Machine Manager, Intrusion Detection System, Intrusion Prevention System, Cloud Let, Multiple Clouds

1. Introduction

Cloud computing is the resource pool where end users can make use of any services through the cloud based data centre. Cloud vendor will provide all the services which are needed for the cloud user based on 'Pay-as-you-go' model. Cloud offers 'Everything-as-a-service (XaaS)' to its customers. However, cloud supplies all kind of services, still the end-user level security problems need to be completely solved. In initial stage intruders are tried to hack the user application and their confidential resources. Later on, intruders are attempted to hack the entire virtual machine and hypervisor where all the user applications are running on it. The key idea behind this proposed work is, in multiple clouds environment it is possible to control all the applications, user resources, secret information and other confidential user process level information are protected with the help of serverless computing. In serverless computing for all the client level process there is an end point which can be provided for accessing and controlling the user services and processes based on key process area (KPA). The main objective is, for the multiple clouds platforms how to secure the user transactions and other customers based service level information.

2. Related Work

As per an author, M. King; M. Muehlemann, "Transforming the reliability, security and scalability of IT communications through the pervasive deployment" stated that, the pervasive deployment of P2P technology brings new opportunities, goal setting factor. This paper reviews how P2P technology can be applied pervasively to provide a

lower cost of network. This paper has applied into three part such as, user application, service connectivity via network and management. This work not focused about the cloud user level security aspect. [1]

An author Nilton Bila, Paolo Dettori et.al, "Leveraging the serverless architecture for securing linux containers" stated that, to secure a linux containers present in the lightweight solution based application packages and its security images need to be iterated in the isolated environment. Vulnerable that might cause the running user service at any time. This approach can safeguard user application against the potential threats in the linux environment. [2]

Author Collins Mtita, Maryline Laurent et.al, "Serverless lightweight mutual authentication protocol for small mobile computing devices", this paper has reviewed the security services over the mobile computing devices by using of AVISPA tool. This approach has only considered the lightweight process, application, services with the presence of mutual authentication protocol. [3]

So, from above literature study reports it is proved that, serverless computing has applied into the various application specific domains. This proposed work will evaluate the security credentials over the multiple cloud service environments by using the serverless computing technique.

3. Proposed Work

Serverless is an approach that mainly addresses the infrastructure and software architecture issues in order to manage the computing resources. It leverages the third party services and API's. User may create the security architectures / security patterns to enable security transactions over the multiple cloud platforms. Serverless computing will work on the fashion of function-as-a-service (FaaS). The major consideration factor in this approach is, establishing the client level security operations should run on the secured cloud platform. User services, applications and other confidential information are protected against the threats in the service provider end. Through this, serverless technique, the machine will customize which user application runs on data centre and also controls the corresponding virtual machine. It will create the strong security layer and define the user level security application parameters.

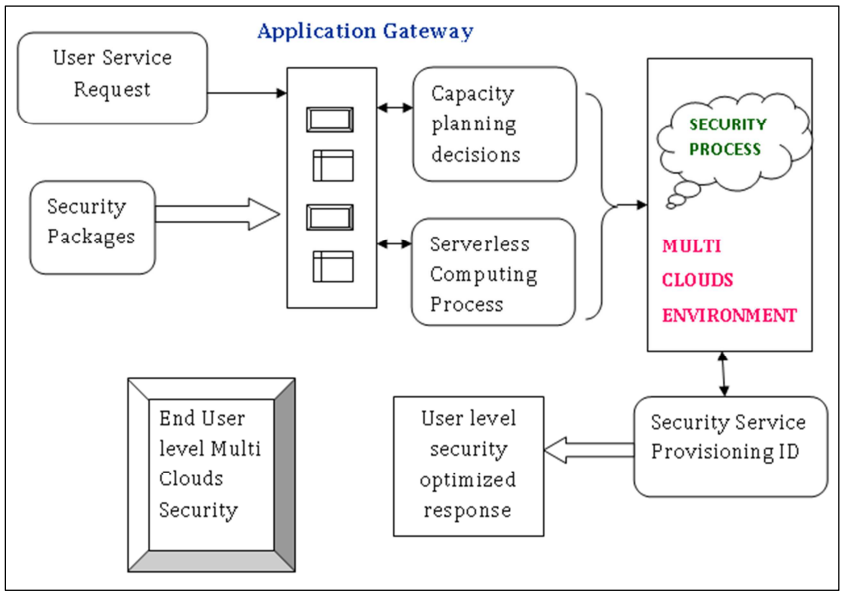

Figure 1. *Proposed System Architecture.*

An above figure 1 will illustrates the functional components of proposed model work. The novelty approach of proposed work is to ensure the security packages, security functional modules and other security parameters which enabled on the multi cloud environment. This process can specify the serverless computing operational values.

The list of user level security based consideration factors are listed below:

1. User service / service (or) application type
2. Location of service request
3. Enabling services from the cloud vendor end
4. Service provisioning model ID
5. Data centre based resource offering
6. Security parameters control
7. Service access from the multiple clouds
8. Serverless computing node

The traditional service computing models enables the security functions based on the access component and the service API's used in the service provider and customer end. The lots of security peripherals can be adapted for the security functions like finding the frequent service request, location where they are using the same type of service access, type of service error, service interruption if any.

Algorithm Used

To prove the user security implication strategy is the most vital part of service emulation processed in the cloud service access environment. To perform the desired tasks in the cloud vendor end, customers can prefer the 'SOC' [security

operation centre].

Classifying the cloud user is the most vital task in the cloud developer end. However, user will identified as a frequent user or normal user which used to determine the behavioural activities and find out the involvement in attack actions. Classification and clustering algorithms are used to evaluate the security performance over the multi cloud platform. In general, classification applies to the user and service usage based sequences. Classification is the most common phenomenon, which can be applied to the resource pool environment whoever using the service with more protection based parameters. In the proposed work, classification algorithm will perform the following tasks:

1. Analyze the user region
2. Service interval time
3. Resource sharing with the other parties
4. Finding the security images applied for the each clients
5. Check the frequency of service usage from the same data centre.
6. Determine the network error or server error in the specified location

With above credentials, the user will create their own security pattern to process the confidential process and its information in a secured environment. The various security components can be used to perform on the multi cloud environments like how many data centre's are currently enabled, easy access cloud vendor location and so forth. In this strategy, the clustering algorithm will operate the following functions:

1. After partitioning the user group, collect the same set of user groups
2. Cluster center can be formed
3. User identification can be verified with the registered cloud user group
4. Multi cloud user groups to be analyzed the intruder's entry.
5. Check the security pattern and service access pattern can be defined differently
6. Enable security check operation in all the data centre locations.

4. Implementation Work & Results

To process the security parameters and its implications need to be iterated in the service access platform. To isolate the process of multi cloud user groups can be associated with the corresponding cloud vendor location. Serverless computing mechanism will operate on the no virtual machine, no dedicated cloud server. All the controls can be specified and processed with the suitable KPA (Key process area) and API's. Serverless computing model works on the principle of 'stateless' mechanism and it will considered to the user group entities. Entire set of access contents can be iterated in the cloud user end. The following formula's can be used to specify the outcomes of security performance.

$$\text{Security performance rate} = \frac{\text{Number of cloud user applications runs on the multi cloud} + \text{Service usage}}{\text{Attacks rate (\%)}}$$

Multi cloud environment operates functions under 'n' number of user groups that can be defined in the service processing applications. Form this final throughput value can be identified.

Throughput Efficiency on multi clouds = Security performance rate / 100

Based on the user centric datasets can be taken into the operational sequences on multi cloud environments to analyze the security service and also upgrading the service provisioning values. To indicate the various security constraints that can be evaluated based on the service usage rate by the individual users. The following the table results are obtained during the cloud simulation time.

Simulation Environment Setup:

Cloud simulator type: Cloudlet – middle 3 - tier hierarchy

Platform used: Java JDK 1.7

OS: Windows 8 / XP / advanced

OS bit: operated on 64 bit host.

Controller type: cloud host controller

Table 1. *Dataset and its Process.*

Data Centre Location (DC)	Type of Dataset	Service Migration Time (ms)
DC – 21	Numerical dataset	0.004
DC - 709	Text dataset	0.87
DC - 83	Graphical dataset	0.201
DC - 152	Alphanumeric dataset	0.0531

An above table 1 illustrates the process of finding the suitable data centre location where the cloud resources are optimized and to process the distinct types of datasets its need to identify the service migration time which required completing the security performance on the multiple clouds environment.

Table 2. *Analyzing the Security Performance in Multi Clouds.*

Serverless Access Environment Processed Status	Service Migration Time	Security Parameter Type	Security Performance Rate (%100)
Iterated	0.004	OAuth	87.93
Defined	0.87	OpenID	89.02
Optimized	0.201	VirtID	92.64
Processed	0.0531	OAuth	98.48
Processed	0.183	OAuth	98.90

Table 3. *Determining the Throughput Value.*

Serverless Enabled Device status	Multi cloud user group region (GR)	Throughput Efficiency (%100)
Operated	GR – 1093	99.93
Indicated	GR – 71	87.02
Not operated	GR – 8934	42.4
Queued	GR – 0625	67.94

From above tables 2 and 3 will depicts the functional process of examining the security level performance on the multi cloud platform. In serverless computing all the functional modules and its blocks can be segmented as a various parameters and it will justify the user group regions whoever using the cloud services and resources in a frequent manner.

5. Experimental Graphs

After the computations of implementation process, the multi clouds environment has set the security credentials for increasing the security level performance via serverless computing. The entire process has been optimized and controlled by a VMM and safeguard the user centric applications and their data from the intruders. The following diagram will shows the analytical and experimental outcomes of the proposed approach which is depicted below:

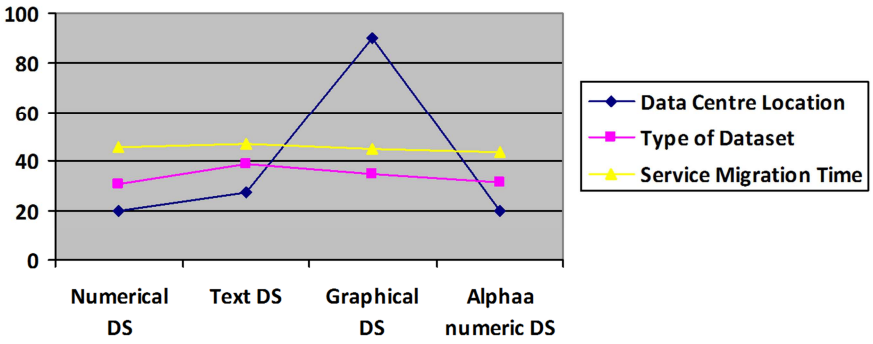

Figure 2. *Processing distinct types of datasets in Multi clouds.*

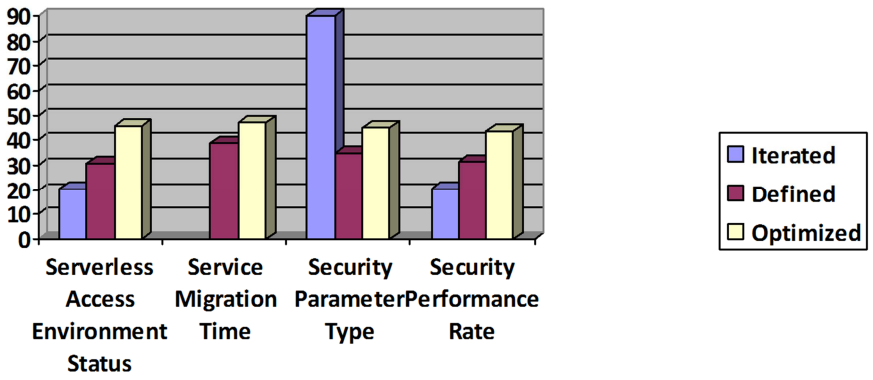

Figure 3. *Analysis Outcomes of Security Performance.*

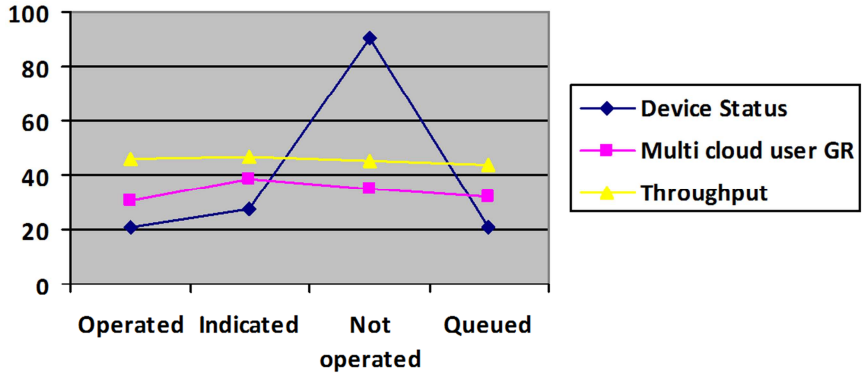

Figure 4. *Illustration of Multiclouds performance outcome.*

From above figures 2, 3 and 4 will depicts the functional flow of the serverless computing operational values. How the multi clouds are enabled in the improvement of cloud user security services. The distinct types of process, security

parameters and access control segments are monitored and optimized in the cloud environment. So, that the rest of the security packages are enable the self-controlling segments to operate on the client end location.

6. Conclusion

The serverless computing models can operate on the different multi clouds vendor which can be accessed via a control segment. From the implementation model, all the resources, security components, access segments are optimized in the public cloud environment. So, any user they can prefer the serverless computing approaches to improve the security level performance on the client end locations.

Future Enhancement

From analyzing the application specific domain operations, all the security level components are incorporated in the cloud computing environment. This type of serverless computing approaches can be preferred and applied into the bigdata, IOT security platforms to enhance the security level performance outcome.

References

[1] M. King, M. Muehlemann, "Transforming the reliability, security and scalability of IT communications through the pervasive deployment of serverless software infrastructure", IEEE Journal on peer-to-peer computing, ISBN: 0-7695-1810-9, 2002.

[2] Nilton Bila, Paolo Dettori et.al, "Leveraging the Serverless Architecture for Securing Linux Containers", Published in: Distributed Computing Systems Workshops (ICDCSW), IEEE International Conference on Distributed computing systems, ISSN: 2332-5666, 2017.

[3] Youngioo Shin, Dongyoung Koo et.al, "SEED: Enabling Serverless and Efficient Encrypted Deduplication for Cloud Storage", IEEE international conference on Cloud Computing Technology and Science (CloudCom), ISSN: 2330-2186, 2016.

[4] Collins Mtita, Maryline Laurent et.al, "Serverless lightweight mutual authentication protocol for small mobile computing devices", International Conference on New Technologies, Mobility and Security (NTMS), ISSN: 2157-4960, 2015.

[5] Sheikh I. Ahamed, Farzana Rahman et.al, "S3PR: Secure Serverless Search Protocols for RFID", International Conference on Information Security and Assurance, ISBN: 978-0-7695-3126-7, 2008.

[6] Poornima, B.; Rajendran, T, "Improving Cloud Security by Enhanced HASBE Using Hybrid Encryption Scheme", Computing and Communication Technologies (WCCCT), 2014 World Congress on march-14.

[7] Durrani, A, "Analysis and prevention of vulnerabilities in cloud applications", Information Assurance and Cyber Security (CIACS), 2014 IEEE Conference on 2014.

[8] Chang Liu; "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates Parallel and Distributed Systems", IEEE Transactions on cloud computing - 2014.

[9] Hussain, M.; "Effective Third Party Auditing in Cloud Computing", International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2014.

[10] Vikas Saxena, et.al, "Implementation of a secure genome sequence search platform on public cloud-leveraging open source solutions", Journal of Cloud Computing: Advances, Systems and Applications 2014.